**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**

| | |
|---|---|
| ELENA TREBAOL LINDEKUGEL, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>STRAFFORD PUBLICATIONS, LLC and BARBRI, INC.,<br><br>Defendants. | Civil Action No. _____<br><br>**CLASS ACTION**<br><br>**DEMAND FOR JURY TRIAL** |

# CLASS ACTION COMPLAINT

## INTRODUCTION

Elena Trebaol Lindekugel ("Plaintiff"), individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to themselves or their counsel, which are based on personal knowledge.

## NATURE OF THE CASE

1. Plaintiff brings this action to redress Defendant Strafford Publications, LLC ("Defendant Strafford") and Defendant Barbri, Inc.'s ("Defendant Barbri") (collectively, "Defendants") practices of knowingly disclosing Plaintiff's and its other customers' identities as well as the identities of the prerecorded video materials to which they purchased access on Defendants' www.straffordpub.com website (the "Website") to third parties in violation of the federal Video Privacy Protection Act ("VPPA"), 18 U.S.C. § 2710.

2. Over the past two years, Defendants have systematically transmitted (and continue to transmit today) its customers' personally identifying video viewing information to Meta Platforms, Inc. ("Meta"), formerly known as Facebook, Inc. ("Facebook"), using snippets of code called a tracking pixel.

3. Defendants knowingly and intentionally transmitted this personally identifying video viewing information to Meta.

4. In the simplest terms, the tracking pixel installed by Defendants captures and discloses to Meta information that reveals the specific video materials that a particular person requested or obtained on Defendants' Website (hereinafter, "Private Video Information").

5. Defendants disclosed and continue to disclose its customers' Private Video Information to these third parties without asking for, let alone obtaining, its customers' consent to these practices.

6. The VPPA clearly prohibits what Defendants have done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of $2,500.00, *see id.* § 2710(c).

7. Accordingly, on behalf of themselves and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendants for intentionally and unlawfully disclosing their Private Video Information to third parties.

## PARTIES

### I. Plaintiff Elena Trebaol Lindekugel

8. Plaintiff is, and at all times relevant hereto was, a citizen and resident of Seattle, Washington.

9. Plaintiff goes by the name "Elena Trebaol" for professional purposes.

10. Plaintiff has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

11. Within the past two years, Plaintiff purchased several video on-demand continuing legal education ("CLE") courses on Defendants' Website, which provided her access to prerecorded video materials.

12. Plaintiff provided her name and email address in association with the purchase of these materials.

13. Plaintiff purchased the prerecorded video materials on Defendants' Website during the time frame applicable to this case. Accordingly, Plaintiff requested or obtained, and is therefore a consumer of, prerecorded video materials sold by Defendants on their Website.

14. At all times relevant hereto, including when purchasing access to prerecorded video materials from Defendants on their Website, Plaintiff had a Facebook account, a Facebook profile, and an FID associated with such profile.

15. At all times relevant hereto, including when purchasing access to prerecorded video materials from Defendants on their Website, Plaintiff's Facebook profile was set to public status such that her name and photograph associated with the account was publicly accessible.

16. Plaintiff watched the prerecorded videos she purchased access to on Defendants' Website while logged into Facebook during the last two years.

17. When Plaintiff purchased access to prerecorded videos from Defendants, Defendants disclosed to Meta Plaintiff's FID coupled with a URL identifying the prerecorded video materials she purchased, among other information about Plaintiff and the device she used to make the purchase

18. Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendants to disclose her Private Video Information to Meta.

19. Because Defendants disclosed Plaintiff's Private Video Information to Meta during the applicable statutory period, Defendants violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

## II. Strafford Publications, LLC

20. Defendant Strafford is a Delaware limited liability company.

21. Defendant Strafford has with a principal office address of 12222 Merit Drive, Suite 1340, Dallas, Texas 75251.

22. Defendant Strafford has a principal record address of 590 Dutch Valley Road, Atlanta, Georgia 30324.

23. Defendant Strafford is registered to do business within the State of Georgia and may be served through its registered agent, Corporation Service Company, 2 Sun Court, Suite 400, Peachtree Corners, GA 30092.

24. Defendant Strafford conducts business within the jurisdictional boundaries of this district, including by operating an office at the address 590 Dutch

Valley Road, Atlanta, Georgia 30324, maintaining employees in this district, and offering its products for sale to consumers in this district.

25. Defendant Strafford, along with Defendant Barbri, operates the Website www.straffordpub.com, which offers for sale access to various prerecorded videos containing CLE and continuing professional education ("CPE") content.

## III. Defendant Barbri, Inc.

26. Defendant Barbri is a Delaware limited liability company.

27. Defendant Barbri has with a principal office address of 12222 Merit Drive, Suite 1340, Dallas, Texas 75251.

28. Defendant Barbri is registered to do business within the State of Georgia and may be served through its registered agent, Corporation Service Company, 2 Sun Court, Suite 400, Peachtree Corners, GA 30092.

29. Defendant Barbri conducts business within the jurisdictional boundaries of this district, including through the operations of its wholly-owned subsidiary, Defendant Strafford. Defendant Barbri further maintains employees or subcontractors within the boundaries of this district and sells products, including bar exam review courses, to consumers in this district.

30. Defendant Barbri, along with Defendant Strafford, operates the Website www.straffordpub.com, which offers for sale access to various prerecorded videos containing CLE and CPE content.

## JURISDICTION AND VENUE

31. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

32. Personal jurisdiction is proper because Defendants transact business, maintain employees or contractors, sell their products to consumers, advertise their products to consumers, and deliver their products to consumers, within this judicial District.

33. Venue is proper because a substantial part of the events of omissions giving rise to the claim occurred in this district.

34. Personal jurisdiction and venue are also proper in this judicial District because the Terms of Use on Defendants' Website provide "any action arising out of or relating to these terms shall be filed only in state or federal courts located in the City of Atlanta, County of Fulton, State of Georgia."

## VIDEO PRIVACY PROTECTION ACT

35. The VPPA prohibits companies (like Defendants) from knowingly disclosing to third parties (like Meta) information that personally identifies consumers (like Plaintiff and the putative class members) as having requested or obtained particular videos or other audio-visual materials.

36. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such

provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

37. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sen. Simon). Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." *Id*. at 8 (statement of Sen. Leahy).

38. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy

protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id*.

39. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[1]

40. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure

[1] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[2]

41. In this case, however, Defendants deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously) disclosing their Private Video Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

## BACKGROUND FACTS

### I. Consumers' Personal Information Has Real Market Value

42. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[3]

---

[2] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

[3] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

43. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[4]

44. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

45. In fact, an entire industry exists where companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

46. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age,

---

[4] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

[5] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[6] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

47. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[8]

48. Recognizing the severe threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[9]

---

[7] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more.

[8] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c.

[9] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), available at https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

49. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendants share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[10]

50. Defendants are not alone in violating their customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

## II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

51. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

[10] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

52. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[11] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[12]

53. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[13]

54. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to

[11] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[12] *Id*.

[13] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[14]

55. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[15] As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

## III. Defendants Are Video Tape Service Providers

56. Defendants sell access to prerecorded video materials to consumers on the Website (www.straffordpub.com).

57. These materials include thousands of hours of prerecorded videos. The videos offered for sale by Defendants fall into two primary categories: (1) CLE courses designed to help lawyers meet their continuing education professional requirements and (2) CPE courses designed to help accountants meet their continuing education professional requirements.

---

[14] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy* (Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[15] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

58. Defendants offer various formats for these video materials. One format is so-called "on-demand" videos, which are prerecorded videos of continuing education presentations. An example is pictured below:


59. The URLs of the webpages where these prerecorded videos are available for sale on the Website contain the names of the videos offered for sale on that page. For example, the URL for the above-picture video, entitled "Survey of U.S. State Privacy Laws: Common Themes, Key Differences, Compliance Strategies, Risk Mitigation" is: https://www.straffordpub.com/products/survey-of-u-s-state-privacy-laws-common-themes-key-differences-compliance-strategies-risk-mitigation-2024-09-18.

60. Once a consumer purchases access to a prerecorded video on the Website, the consumer can access and watch the video at any time through a portal on the Website.

61. Accordingly, Defendants are each a "video tape service provider" within the meaning of 18 U.S.C. § 2710.

## IV. Defendants Use the Meta Pixel on the Website to Systematically Disclose Their Customers' Private Video Information to Meta

62. A tracking pixel is a piece of JavaScript code added to a website as a graphic element that is loaded when a user arrives at the website hosting the pixel.

63. When a user visits a website which has tracking pixels enable, an instance of the tracking pixel loads in the HTML code of the page on the user's web browser.

64. Sometimes, a cookie corresponding to the tracking pixel already exists in the browser. In those cases, the cookie contains a unique ID that follows the user of the internet browser from web page to web page, and that cookie connects with the tracking pixel.

65. In other cases, a cookie corresponding to the cookie does not exist on the browser. In those cases, a unique ID is created and saved in a cookie.

66. After identifying the corresponding cookie (with its unique ID), the tracking pixel's embedded URL points to a third party's (e.g., Meta) designated tracking URL and reports to the third party the user's activity for the duration of the

visit, along with the unique ID stored in the cookie which identifies the specific web user.

67. To implement a tracking pixel, a website administrator must place the base tracking pixel code in the website's JavaScript code. That code acts as an initiator for the tracking pixel's behavior. Once initiated, the code will load a library of functions (e.g., fbevents.js for the Meta Pixel) that enable to pixel to respond to certain actions taken by the user of the internet browser and initiate data transmissions regarding the user (e.g., sending query string parameters and cookie values) to the third-party's tracking URL.

68. Defendants have installed and programmed tracking pixels from at least Meta and Pinterest on the Website and uses these pixels to transmit the Private Video Information of its customers to those third parties in violation of the VPPA.

**A. The Meta Pixel**

69. Defendants have disclosed the Private Video Information of its customers to Meta using a snippet of programming code called the "Meta Pixel," which Defendants installed and configured on the Website.

70. The information that Defendants disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the identity of the specific prerecorded video material that each of its customers requested or obtained through the Website.

71. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person, such as their photographs, contact information, employer, etc.).

72. Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. When someone has access to an individual's FID, they are able to precisely identify that individual person.

73. As alleged below, whenever a person with a Meta account purchases prerecorded video material on Defendants' Website, the Meta Pixel technology that Defendants intentionally installed on the Website transmits the customer's Private Video Information (e.g., their personally identifying information and the specific video materials they requested or obtained) to Meta – all without the customer's consent, and in clear violation of the VPPA.

74. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta."[16] Meta is now the world's largest social media platform. To

[16] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.

create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

75. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendants, Meta, and third-party marketing companies to build detailed profiles about websites' customers and serve them with highly targeted advertising.

76. A Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."[17] This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[18] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

[17] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.

[18] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

77. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[19]

78. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[20]

79. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website visitors to Meta.

80. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[21]

81. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] . . . as well as to combine those user IDs with corresponding Event Data."[22]

---

[19] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[20] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms.

[21] *Id*.

[22] *Id*.

82. The Business Tools Terms define "Event Data" as, *inter alia*, "information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[23]

83. A list of 'Standard Events' which can be captured on a website with the Meta Pixel enabled, and then transmitted to Meta and logged is available on Meta's website. Among the standard events are:

- Complete Registration: Submitting information in exchange for a service provided by your business. For example, signing up for an email subscription.
- Initiate Checkout: The start of a checkout process. For example, clicking a checkout button.
- Lead: A submission of information by a customer with the understanding that they may be contacted at a later date by your business. For example, submitting a form or signing up for a trial.
- Schedule: The booking of an appointment to visit one of your locations.[24]

84. The Meta Pixel can also be used to transmit data collected on forms which appear on a website to Meta, including the following form fields: First Name,

[23] *Id*.

[24] Meta, "Specifications for Meta Pixel Standard Events," available at https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

Last Name, Phone, Gender, Birthdate, City, State or Province, Zip or Postal Code, Country.[25]

85. Website operators use the Meta Pixel to send information about visitors to their websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the URL of the webpage triggering the transmission.

86. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta.

87. Defendants have configured the Meta Pixel on its Website to send Event Data to Meta.

88. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the URL of the website, or the Event Data.

89. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.[26]

90. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to "track [] the people and type of actions they

[25] Meta, "Advanced Matching – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/advanced/advanced-matching.

[26] *See id.*

take,"[27] including, as relevant here, the specific prerecorded video material that they purchase or view on the website.

91. The Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

92. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

93. Defendants knowingly use the Meta Pixel to transmit the Private Video Information of its customers to Meta.

94. Whenever a person with a Meta account purchases prerecorded video materials on the Website, Defendants use – and have used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase as well as information identifying the prerecorded video materials requested or obtained from Defendants.

[27] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

95. Defendants use the Meta Pixel to transmit its customers' FID and the URL of each page in the Website's check-out flow to Facebook. The URLs transmitted to Meta during this process identify the video materials requested or obtained by the consumer.

96. For example, when an individual purchases access to the video on-demand "Survey of U.S. State Privacy Laws" on the Website, they begin the checkout process on this page (previously pictured above):[28]

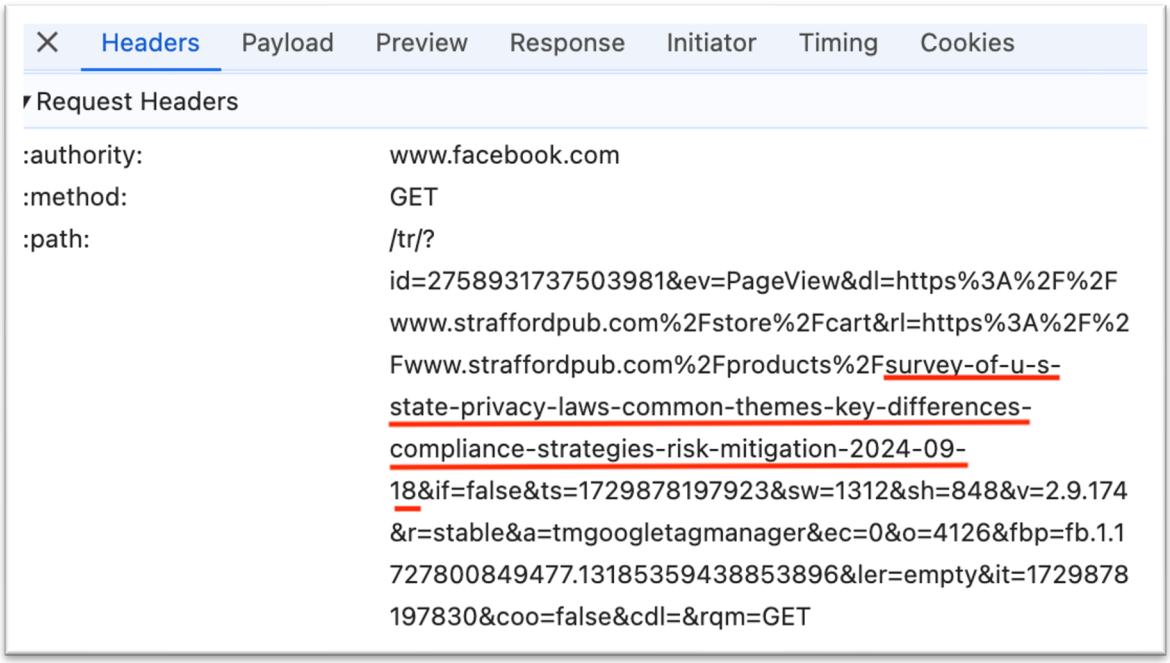

97. When the customer arrives on this page, their FID and the page's URL are transmitted to Meta by Defendants via the Meta Pixel.

[28] Strafford, "Survey of U.S. State Privacy Laws," available at https://www.straffordpub.com/products/survey-of-u-s-state-privacy-laws-common-themes-key-differences-compliance-strategies-risk-mitigation-2024-09-18.

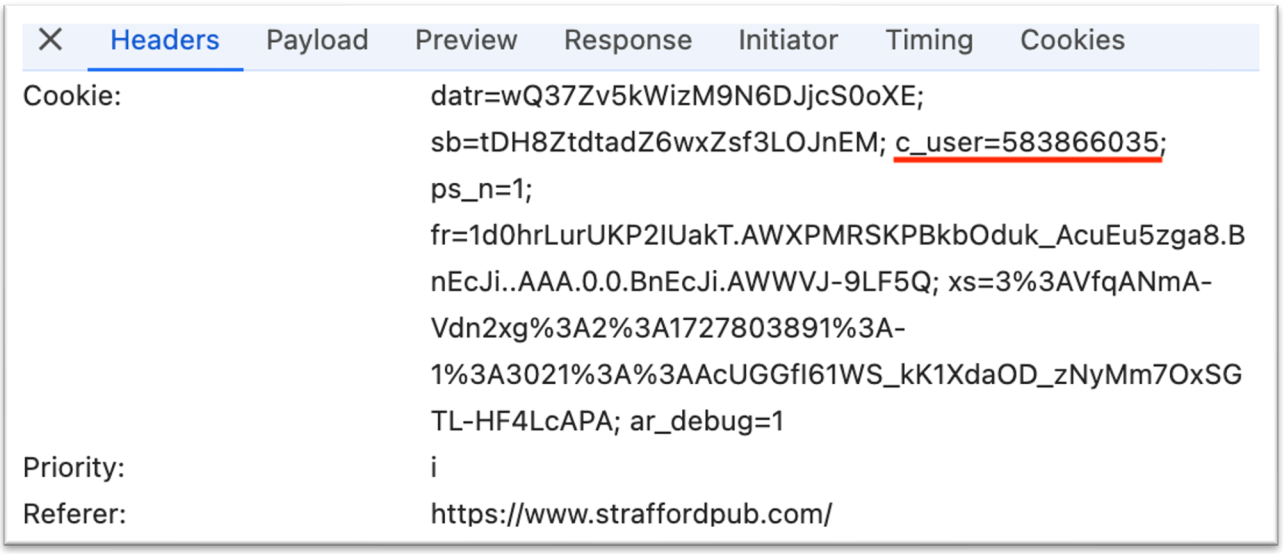
98. When a customer clicks the "BUY CLE ON-DEMAND" button on this page, they are brought to a new page displaying their "Shopping Cart." An example of this page is pictured below:


99. When a consumer arrives on this page (or any similar "Shopping Cart" page), Defendants send the consumer's FID and the name of the prerecorded video content the consumer is requesting to Meta through the operation of the Meta Pixel.

100. Specifically, the Meta Pixel executes a GET Request and then sends the name of the video which is in the consumer's "shopping cart" to Meta, as pictured in the following screenshot (underlining added for emphasis):



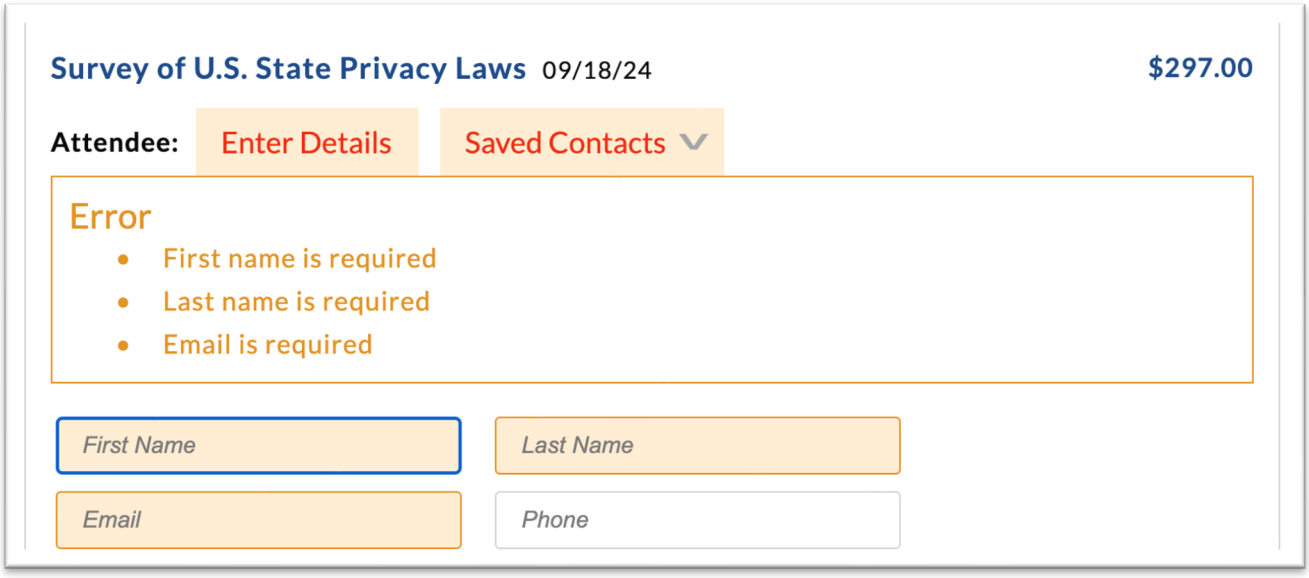

101. In the same transmission, Defendants also send the consumer's FID to Meta. The consumer's FID is embedded in the "c_user" cookie value which Defendants send to Meta. As operating on Defendants' website, and example of this transmission is pictured below (underlining added for emphasis):



102. After receiving this transmission from Defendants, Meta takes these two pieces of information to build consumer profiles of the visitors to Defendants' Website. Using Meta's Business Tools, Defendants (and other advertisers) are then able to track the visitors across the internet and serve them targeted advertising which aligns with their interests and online activities as collected and compiled by Meta.

103. Further, Defendants use the "Event Data" capabilities of the Meta Pixel to transmit even more detailed Private Video Information to Meta from throughout the checkout process on the Website.

104. When users click "Checkout" on the "Shopping Cart" page, they are prompted to enter their name, email address, and phone number, as pictured in the following screenshot:




105. When users click "Save This Attendee" after entering at least their name and email address, the Website sends the name and email address (and also the

phone number, if that is entered) to Meta using the Meta Pixel's 'Event Data' capabilities (including, but not limited to, through the operation of the Meta Pixel's "fbevents.js:204" code)

106. When the consumer clicks "Place Order" at the end of the checkout flow, Defendants send the consumer's name, contact information, FID, and the name of the rerecorded video to which they purchased access to Meta through the operation of the same GET requests and Event Data transmissions.

107. Defendants intentionally installed the Meta Pixel on the Website, knowing and intending to make these transmissions.

108. In this way, among other methods, Defendants knowingly discloses to Meta the Private Video Information of its consumers.

109. Plaintiff has purchased access to prerecorded video materials on Defendants' Website while logged into Facebook during the last two years. Accordingly, Defendants have transmitted Plaintiff's identity and the fact that she requested or obtained prerecorded video material to Meta during the last two years.

110. Defendants intentionally programmed the Website to include the Meta Pixel code in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta. In doing so, Defendants knew that the Website would transmit its customers' Private Video Information to Meta.

111. Once the Meta Pixel code is installed on a website, the website operator can access a dashboard on www.facebook.com to track website visitors'

activities on the website, including Event Data, and to deliver targeted ads to those visitors on Meta's various internet properties.

112. Defendants intentionally installed the Meta Pixel and transmitted the Private Video Information of Plaintiff and the putative class members to Meta in order to take advantage of these internet tracking, marketing, and advertising services offered by Meta.

113. The Meta Pixel code systematically transmits to Meta the FID of each person with a Meta account who requests or obtains prerecorded video material on the Website, along with URLs and other data identifying the prerecorded video materials that the person requested or obtained.

114. With only a person's FID and the identity of the prerecorded video material requested or obtained (or URL where such material is available)—all of which Defendants knowingly provide to Meta on a systematic basis—any ordinary person could learn the identity of the person to whom the FID corresponds and identify the specific prerecorded video material that the person requested and obtained. The person's identity can be determined by simply by accessing the URL www.facebook.com/[*insert the person's FID here*]/.

115. Defendants' practice of disclosing the Private Video Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action.

116. At all times relevant hereto, whenever Plaintiff or any other person requested or obtained prerecorded video material on Defendants' Website, Defendants disclosed to Meta (*inter alia*) the specific identity of the video material that was requested or obtained, along with the FID of the person who requested or obtained it (which, as discussed above, uniquely identified the person).

117. At all times relevant hereto, Defendants knew that the Meta Pixel was disclosing their customers' Private Video Information to Meta.

118. Although Defendants could easily have programmed the Website so that none of their customers' Private Video Information is disclosed to Meta, Defendants instead chose to program its Website so that all of its customers' Private Video Information is disclosed to Meta.

119. Before transmitting their customers' Private Video Information to Meta, Defendants failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

120. By intentionally disclosing to Meta Plaintiff's and their other customers' FIDs together with the identity of the video materials that they each requested or obtained, without any of their consent to these practices, Defendants knowingly violated the VPPA on an enormous scale.

## CLASS ACTION ALLEGATIONS

121. Plaintiff seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, purchased access

to video materials on the Website (www.straffordpub.com) and had their Private Video Information transmitted to a third party.

122. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendants.

123. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendants embedded tracking pixels on its Website that monitor and track actions taken by visitors to its Website; (b) whether Defendants reports the actions and information of visitors to third parties; (c) whether Defendants knowingly disclosed Plaintiff's and the Class members' Private Video Information to third parties; (d) whether Defendants' conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiff and the Class members are each entitled to a statutory damage award of $2,500, as provided by the VPPA.

124. The named Plaintiff's claims are typical of the claims of the Class in that the Defendants' conduct toward the putative class is the same. That is, Defendants embedded tracking pixels on their Website to monitor and track actions

taken by class members to its Website and report this to third parties. Further, the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendants' uniform and wrongful conduct in intentionally disclosing their Private Video Information to third parties.

125. Plaintiff is an adequate representative of the Class because she is interested in the litigation; her interests do not conflict with those of the Class members they seek to represent; she has retained competent counsel experienced in prosecuting class actions and intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of all Class members.

126. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision

by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

## CAUSE OF ACTION
## Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

127. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

128. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

129. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendants are each a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because they are engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

130. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and each of the Class members are a "consumer" within the

meaning of the VPPA because they each purchased access to prerecorded video material or purchased prerecorded video material from Defendants' Website that was sold and delivered to them by Defendants.

131. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Private Video Information that Defendants transmitted to third parties constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identifies Plaintiff and the Class members to third parties as individuals who purchased, and thus "requested or obtained," specific prerecorded video materials or a subscription to access prerecorded video materials from Defendants via its Website.

132. Defendants knowingly disclosed Plaintiff's and the Class members' Private Video Information to third parties via tracking pixel technology because Defendants intentionally installed and programmed the tracking pixel code on their Website, knowing that such code would transmit to third parties the identities of the video materials watched by its customers coupled with its customers' unique identifiers (including FIDs).

133. Defendants further knowingly disclosed Plaintiff's and the Class members' Private Video Information to third parties via the pixel tracking technology because Defendants intentionally installed and programmed the pixel tracking code on its Website, knowing that such code would transmit to third parties the purchases

of specific prerecorded video materials requested or obtained by its customers coupled with its customers' unique identifiers (including FIDs).

134. Defendants failed to obtain informed written consent from Plaintiff or any of the Class members authorizing it to disclose their Private Video Information to any third party. More specifically, at no time prior to or during the applicable statutory period did Defendants obtain from any person who purchased prerecorded video material on its Website (including Plaintiff or any of the Class members) informed, written consent that was given in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendants provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

135. By disclosing Plaintiff's and Class members' Private Video Information, Defendants violated their statutorily protected right to privacy in their Private Video Information.

136. Consequently, Defendants are liable to Plaintiff and each of the Class members for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendants Strafford Publications, LLC and Barbri, Inc., as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b) For an order declaring that Defendants' conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiff and the Class and against Defendants on all counts asserted herein;

d) For an award of $2,500.00 to each of Plaintiff and the Class members, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendants from disclosing the Private Video Information of its consumers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Respectfully submitted,

Dated: December 9, 2024

HEDIN LLP

/s/ Eric Funt

Eric Funt
Georgia Bar No. 588961.
The Champion Firm, P.C.
445 Franklin Gateway SE, Suite 100
Marietta, GA 30067
Telephone: 404-495-7459
Facsimile: 404-671-9347
eric@thechampionfirm.com

Tyler K. Somes*
District of Columbia Bar No. 90013925
HEDIN LLP
1100 15th Street NW, Ste 04-108
Washington, D.C. 20005
Telephone: (202) 900-3332
Facsimile: (305) 200-8801
tsomes@hedinllp.com

*Counsel for Plaintiff and Putative Class*

**Pro Hac Vice Motion Forthcoming*